総務省
MIC Ministry of Internal Affairs and Communications

身近に迫るサイバー脅威への対策

総務省情報流通行政局情報セキュリティ対策室
武馬　慎

2011年3月1日

目次

総務省
MIC Ministry of Internal Affairs and Communications

１．情報セキュリティへの脅威の変遷と現状

情報セキュリティへの脅威

ICTの利用には様々な脅威もある。不適切な対応は、金銭的、社会的リスクを伴う。

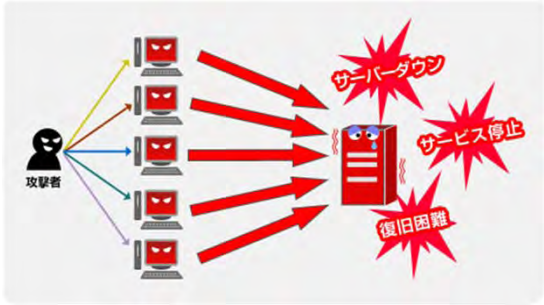
○不正アクセス

・利用する権限を与えられていないコンピュータに対して、不正に接続する行為

・個人情報や機密情報等を盗み出し、ユーザになりすまして不正行為を行ったり、盗み出した情報を売買したりする

○サイバー攻撃

・サーバなどへ大量の通信を発生させる事によるサービス妨害攻撃（DDoS攻撃）など

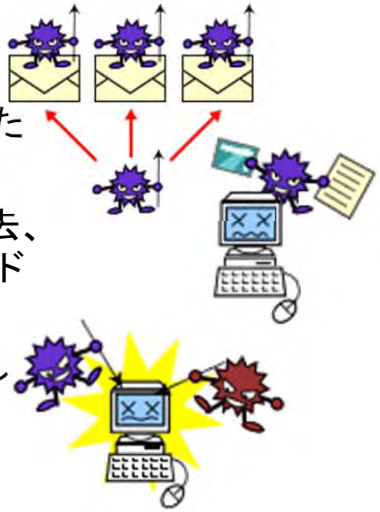


○ウィルス

・コンピュータシステムの破壊や、いたずらを目的とする特殊プログラム

・ハードディスクにあるファイルの消去、コンピュータの起動妨害、パスワードの外部への送信などを行う

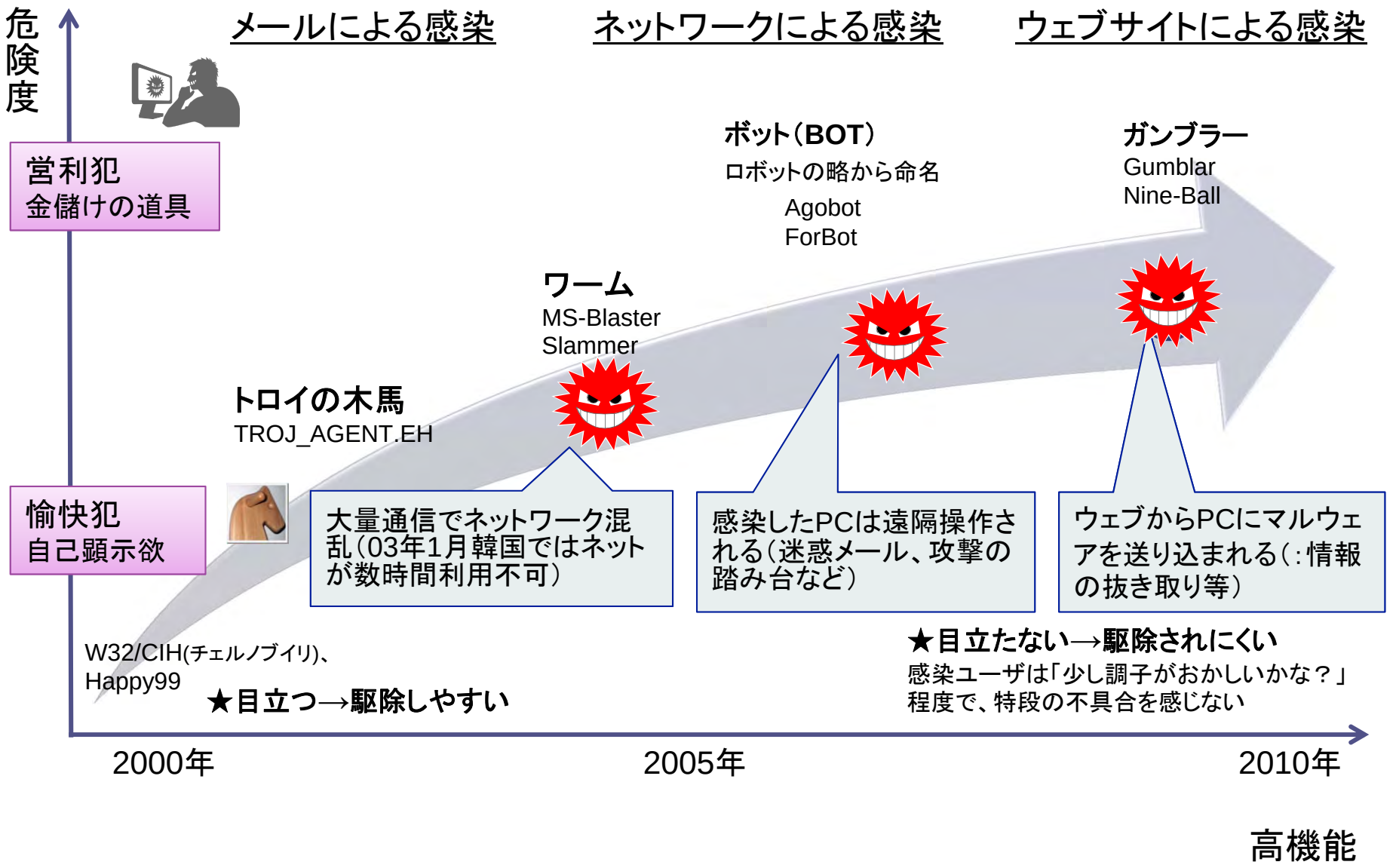
・ネットワークやUSBメモリなどを介して増殖するための仕組みを持つ



○フィッシング詐欺

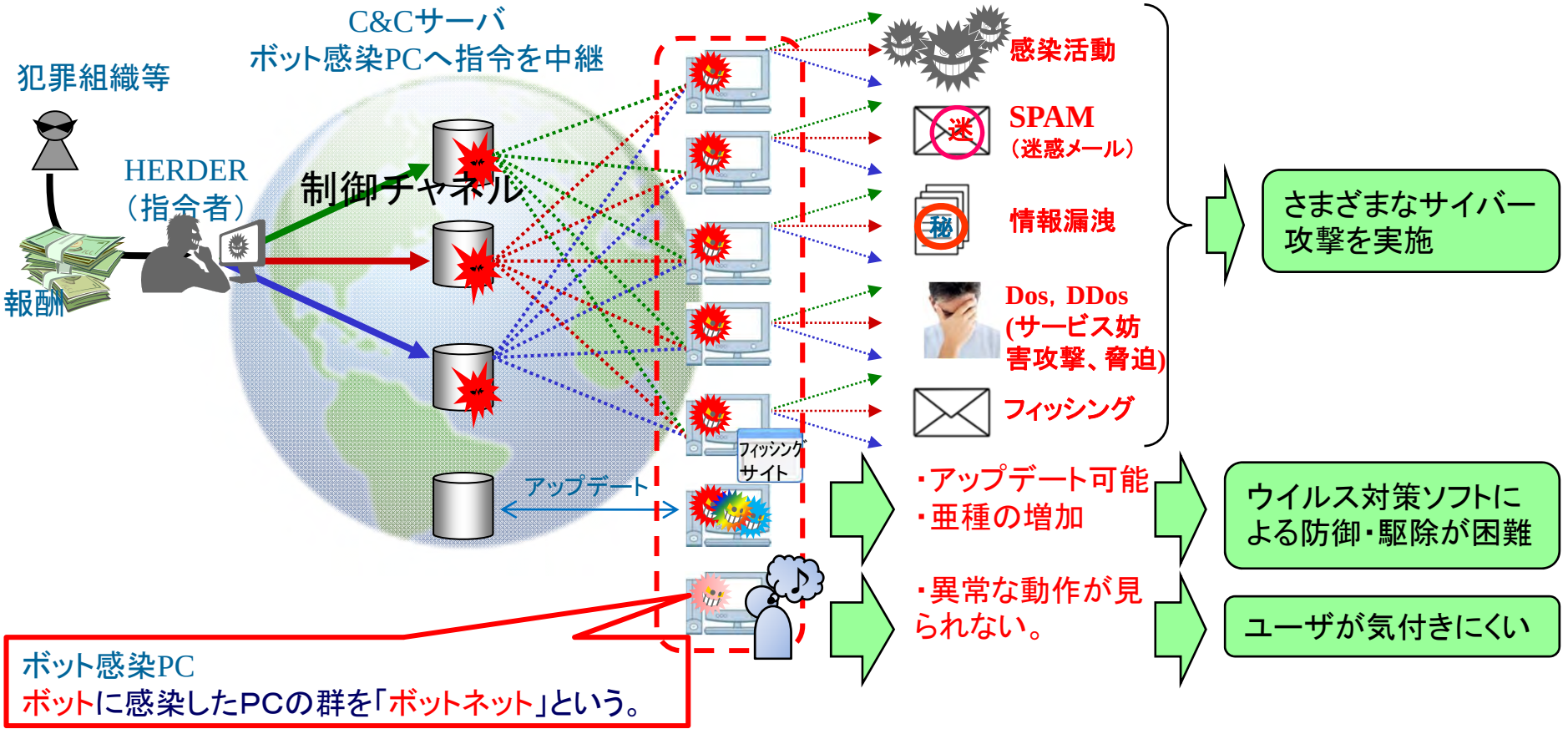
・送信者を詐称した電子メールを送りつけ、偽のホームページに接続させ、偽のホームページから個人情報やクレジットカード番号、ユーザー名、パスワードなどを入手

マルウェアなどの進化・発展



ボットウイルスの脅威

■ボットネットを構築し、悪意の管理者からの命令により、様々なサイバー攻撃を協調して実施。
■命令に従いアップデート（新しいボットプログラムの導入）する機能や、数多くの亜種が存在。
■感染したPCは異常な動作をしているようには見えない。



国家を対象とした大規模サイバー攻撃の例①

2007年5月　エストニア

人口134万人。2004年EU加盟。IT立国を推進し全国民が電子IDカード保有。2007年には世界初のネット国政選挙

- 4月末から約3週間、分散型の業務妨害攻撃（DDoS）等が政府機関や金融機関等に発生
- 政府は対策機器の導入等で対処。一時は、国外からのインターネットを遮断して、収束
- エストニアにあった旧ソ連戦勝記念銅像を撤去する報道に触発されたロシア人の犯行か

2008年8月　グルジア

人口430万人。1991年に旧ソビエト連邦から独立

- 8月8日~10日、分散型の業務妨害攻撃（DDoS）が政府機関を中心に発生。大統領官邸サイトは改ざんされた
- 政府は、重要なサーバの外国への移管、.ru（ロシア）アドレスの通信遮断等で対処
- 同時期のロシアとグルジアの武力衝突を受けたもの。前年のエストニア攻撃と酷似

→ 大統領官邸サイトのトップ画面、大統領の画像にかわりヒトラーの画像が埋め込まれた

国家を対象とした大規模サイバー攻撃の例②

2009年7月　大韓民国

人口4,833万人。ブロードバンド普及率やICT利活用率で世界トップクラス

- 7月7日~10日、国内のウィルス感染PCを中心とした分散型の業務妨害攻撃（DDoS）が政府機関や金融機関等　のシステムに対して発生

区分	被害サイト				統計
	国家/公共機関	金融機関	マスコミ	その他	
1次	大統領府、国会、国防部、外交通商部 ハンナラ党	農協銀行,新韓銀行 韓国外換銀行	朝鮮日報	Auction,Naver	12
2次	大統領府、国会、国防部、国家サイバー安全センター 電子請願G4C	中小企業銀行,ハナ銀行 ウリ銀行,国民銀行	朝鮮日報	Auction,Naver,Daum,Para AlTools,AnLab	15
3次	電子請願G4C	国民銀行	朝鮮日報	*Auction,Naver,Daum,Paran*	7

- 国家情報院（旧KCIA）はサイバー攻撃“注意警報”（5段階中の3段階）発令。北朝鮮による犯行と説明。
- 政府のｲﾝﾀｰﾈｯﾄ・ｾｷｭﾘﾃｨ庁（KISA）は、感染PCのｳｨﾙｽ駆除の呼びかけや、感染PCのネット接続遮断の要請等を実施。
- 推定被害額は27~41億円と見積もられている（：韓国の民間シンクタンク推計）

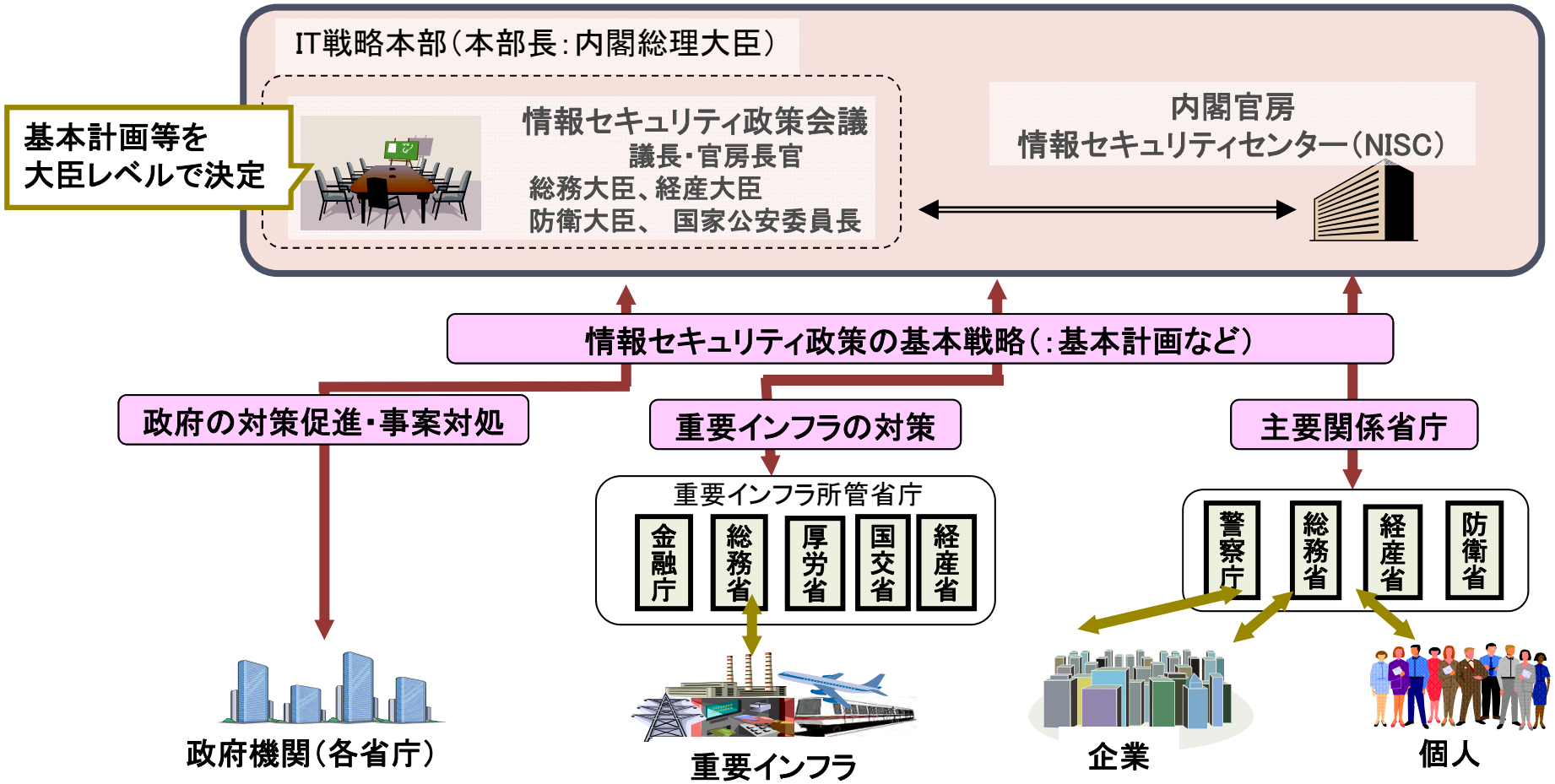
※同時期に、米国の政府機関、金融機関等のシステムに向けて同様の攻撃があるも、特段の被害なし

総務省
MIC Ministry of Internal Affairs and Communications

2．政府における情報セキュリティ政策

情報セキュリティ政策・政府全体の取り組み

- 2005年4月、内閣官房情報セキュリティセンター（NISC；National Information Security Center）設置
- 2005年5月、IT戦略本部の下に「情報セキュリティ政策会議」（議長：内閣官房長官）を設置
- 2006年2月、第一次情報セキュリティ基本計画（情報セキュリティ政策会議決定）
- 2009年2月、第二次情報セキュリティ基本計画（同上）



※重要インフラ：情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流

第２次情報セキュリティ基本計画（2009年～2011年）

「事故前提社会への対応強化」「合理的アプローチ」等を柱に新たな基本計画を策定

	政府・地方公共団体	重要インフラ	企業	個人
対策実施４領域における取組	◆推進体制確立（年次報告書作成・公表等） ◆事業継続性確保の検討、サイバー攻撃等への緊急対応能力強化	◆安全基準の整備等 ◆情報共有体制の強化 ◆セプターカウンシル ◆共通脅威分析、分野横断的演習の実施	◆情報セキュリティ・ガバナンスの促進 ◆対策ツール提供 ◆中小企業の対策促進 ◆コンピュータウィルス等への対応体制の強化	◆ 学校や地域における情報モラル教育の推進 ◆ 個人の質問対応等を行う地域サポータ育成 ◆ サービス提供者のリスク情報等の提供促進
情報提供主体	政府機関統一基準	重要インフラ行動計画	各所管省庁の施策	各省庁の施策

自身の有する情報を預ける主体　：新たな課題として、関係機関等が協力しながら取組みを検討・推進

横断的事項

技術戦略の推進
◆セキュリティ対策の機器・技術開発の推進

情報セキュリティ人材の育成・確保
◆ 保有スキルの見える化、政府の人材育成

国際連携・協調
◆ 脅威把握の官民連携、アジアの知恵結集

犯罪取締まり・保護救済
◆ 犯罪取締りのための基盤整備の推進

新たな情報セキュリティ政策プログラム（2010年～）

現状の課題

大規模なサイバー攻撃事案等の脅威の増大

- ✓ 国境を越えた大規模サイバー攻撃（韓国・米国（2009年7月））、ガンブラー等

急速な技術革新の進展

- ✓ クラウド・コンピューティング技術、IPv6への移行

社会経済活動の情報通信技術への依存度の増大

- ✓ 情報家電、電子タグなどあらゆる機器がネットワークに接続

グローバル化の進展

- ✓ 国境を越えた瞬時の情報流通

「国民を守る情報セキュリティ戦略」（5月11日情報セキュリティ政策会議決定）

国民を守る情報セキュリティ戦略（2010年～2013年）

基本的な考え方（取組みの重点化）

① サイバー攻撃の発生を念頭に置いた政策・対処体制整備
② 新たな環境変化に対応した政策の確立
③ 受動的な対策から能動的な対策へ

- ITリスクを克服し、安全・安心な国民生活を実現
- サイバー空間の安全保障・危機管理政策の強化と情報通信技術政策の連携
- 「安全保障・危機管理」及び「経済」に「国民・利用者保護」を加えた総合的政策
- 国際連携の強化

安全・安心な国民生活を実現

サイバー空間上の我が国の安全保障・危機管理の確保

情報通信技術の利活用を促進し、我が国の経済成長に寄与

実現すべき成果目標

2020年までに、インターネットなど情報通信技術を利用者が活用するにあたっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」に

情報セキュリティ月間

◆ 国民一人ひとりが情報セキュリティについて関心を高め、対応していく必要があるため、情報セキュリティに関する**普及啓発強化**のため、**平成22年、2月を「情報セキュリティ月間」とした。**

具　体　的　な　取　組　の　例

①官房長官メッセージの発信

官房長官から、国民に向け、情報セキュリティの重要性を訴えるメッセージを発信（首相官邸HPに掲載）


首相官邸 Prime Minister of Japan and His Cabinet

官房長官談話等

トップページへ

トップ

内閣官房長官のメッセージ

「情報セキュリティ月間」について
－ 成熟した情報セキュリティ先進国へ －

本年より、新たに2月1日から1か月間を「情報セキュリティ月間」と定めました。

情報通信技術は、社会経済活動や日常生活のあらゆる場面で利用されており、私たちの暮らしの利便性を向上させる重要な社会的基盤となっています。一方で、サイバー攻撃や個人情報流出、重大なシステム障害など情報セキュリティに関する様々な問題が、暮らしや経済に影響を及ぼす可能性が高まっています。

安心・安全にインターネットを使うためには、まず最初に、次のことに気をつけて頂ければと思います。
・ウィルス対策ソフト等を導入し、定期的に更新して最新の状態に保つこと
・基本ソフト（OS）を始め各種ソフトを定期的に更新し、最新の状態に保つこと
・パスワードは、容易に推測できないものとし、他人には知らせないこと

これらを出発点として、情報セキュリティに関する知識を広げて頂ければと思います。国民の皆様一人ひとりが情報セキュリティ対策に取り組むことが、安全で便利な高度情報通信社会を構築することにつながります。

「情報セキュリティ月間」では、国民の皆様に情報セキュリティについての意識を高めて頂くとともに、情報提供の強化などに努めることといたしました。官民が連携して、全国で1,000件を超える関連行事が開催されます。国民の皆様の積極的な御参加を期待しております。

平成22年1月29日
内閣官房長官　平野　博文

インターネット

②セミナー等関連行事の開催

関係省庁、企業等による情報セキュリティ関連のセミナー、講演会等を全国47都道府県で開催

【主な行事の例】

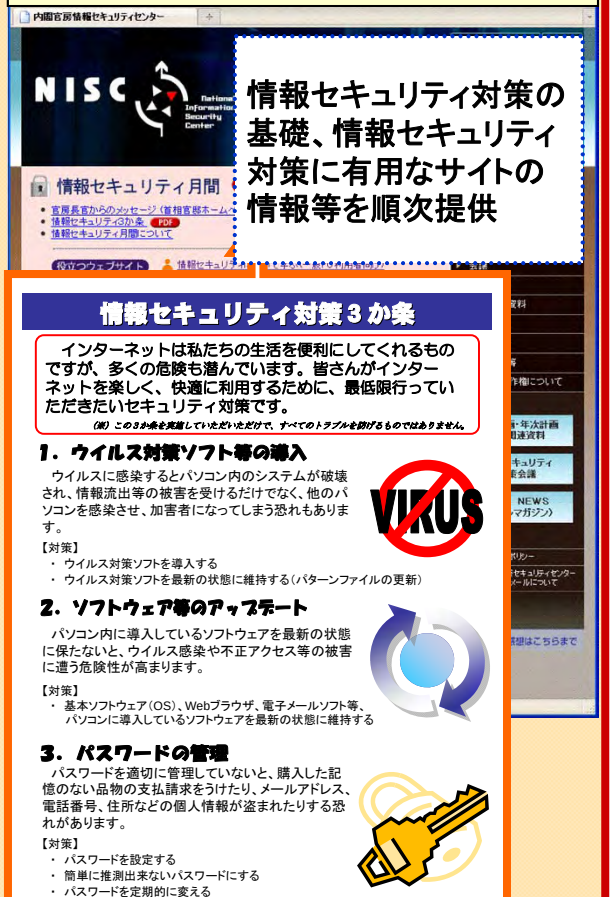
・**情報セキュリティに関する講習等（都道府県警察）**
約2，800件
小中高校等を対象とした、サイバー犯罪の現状、検挙事例等を説明

・**e-ネット安心講座（総務省、文部科学省等）**
約70件
保護者等を対象とした、子供たちをネットトラブルから守るための講座

・**インターネット安全教室（経済産業省等）**
約10件
家庭や学校におけるインターネット利用の基礎知識を学習

など、2月中に合計約2，900件の行事を開催、約35万2千人が参加（←昨年の数字）

③ｳｪﾌﾞｻｲﾄにおける情報提供


内閣官房情報セキュリティセンター

NISC National Information Security Center

情報セキュリティ月間

情報セキュリティ対策の基礎、情報セキュリティ対策に有用なサイトの情報等を順次提供

情報セキュリティ対策３か条

インターネットは私たちの生活を便利にしてくれるものですが、多くの危険も潜んでいます。皆さんがインターネットを楽しく、快適に利用するために、最低限行っていただきたいセキュリティ対策です。

（例）この３か条を実施していただいただけで、すべてのトラブルを防げるものではありません。

1．ウイルス対策ソフト等の導入

ウイルスに感染するとパソコン内のシステムが破壊され、情報流出等の被害を受けるだけでなく、他のパソコンを感染させ、加害者になってしまう恐れもあります。

【対策】
・ ウイルス対策ソフトを導入する
・ ウイルス対策ソフトを最新の状態に維持する（パターンファイルの更新）

VIRUS

2．ソフトウェア等のアップデート

パソコン内に導入しているソフトウェアを最新の状態に保たないと、ウイルス感染や不正アクセス等の被害に遭う危険性が高まります。

【対策】
・ 基本ソフトウェア（OS）、Webブラウザ、電子メールソフト等、パソコンに導入しているソフトウェアを最新の状態に維持する

3．パスワードの管理

パスワードを適切に管理していないと、購入した記憶のない品物の支払請求をうけたり、メールアドレス、電話番号、住所などの個人情報が盗まれたりする恐れがあります。

【対策】
・ パスワードを設定する
・ 簡単に推測出来ないパスワードにする
・ パスワードを定期的に変える

情報セキュリティ・総務省の取り組み

ネットワーク　安全なネットワーク環境

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

◆ISPのセキュリティ団体「T-ISAC-Japan」

・2002年に主要ISPが設立。現会員17社
・内閣NISCの「重要インフラ」対応の中心
（事業者間及び官民連携・情報共有の推進）

◆電子署名法の運用（2001年施行）

・ネットでの安心・安全な利用者の認証の実現　（経産省・法務省と共管）

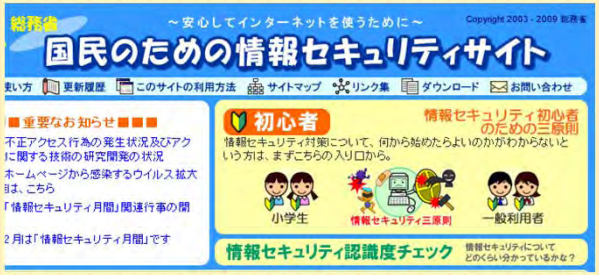
人　利用者の意識向上

◆ユーザに身近な相談相手の育成

・NPO等が取り組む「サポータ育成」を支援

◆ウェブサイトによる情報提供

・国民のための情報セキュリティサイト」



http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm

技術　技術的な対応能力の向上

高度化・多様化するセキュリティ脅威に対応するための研究開発の推進

（情報通信研究機構（NICT）の成果の活用や、 大学・企業への委託研究など）

- ウィルス対策技術
- ネットワーク監視技術
- 暗号技術

国際

二国間連携の強化

多国間会議での連携　APEC, ASEAN, OECD

国際標準化による技術展開　ITU

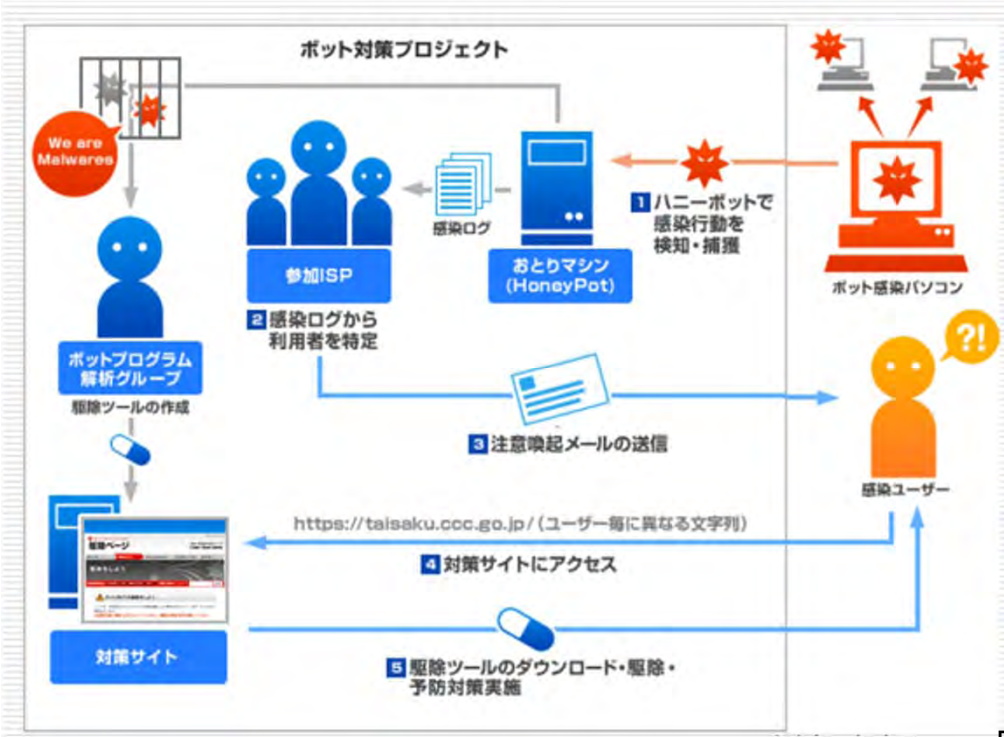
- 情報共有
- 共同プロジェクト実施
- 事業者間交流の促進
- 研究者交流の促進

ボット対策プロジェクト①～概要～

◆ハニーポットを用いて、1日平均25種の新種ボットウイルスを発見し、ウイルス対策ソフトに反映。

◆1日平均438人の感染者を発見し、参加ISP（76社）が感染者にウイルス駆除、WindowsUpdate等の対策実施を勧奨。

◆ウイルス駆除ツールをウェブサイトで提供し、インターネット利用者の自発的なウイルス駆除等の実施をサポート。
（CCCのホームページの1日平均アクセス数：12,722件、駆除ツールの1日平均ダウンロード回数 ：1,110回）



1 ボットウイルスの捕獲

感染PCから行われる感染攻撃を補足しウイルスの捕獲と感染元情報の取得を行う。

2 感染ユーザの特定

感染元情報から感染ユーザを特定する。

3 注意喚起メール（封書）の送信

ユーザに感染を伝えCCCの対策サイトでの駆除・対策を依頼する。
この際に接続アドレスには、個人を識別可能な文字列を挿入し、進捗状況を把握できるようになっている。

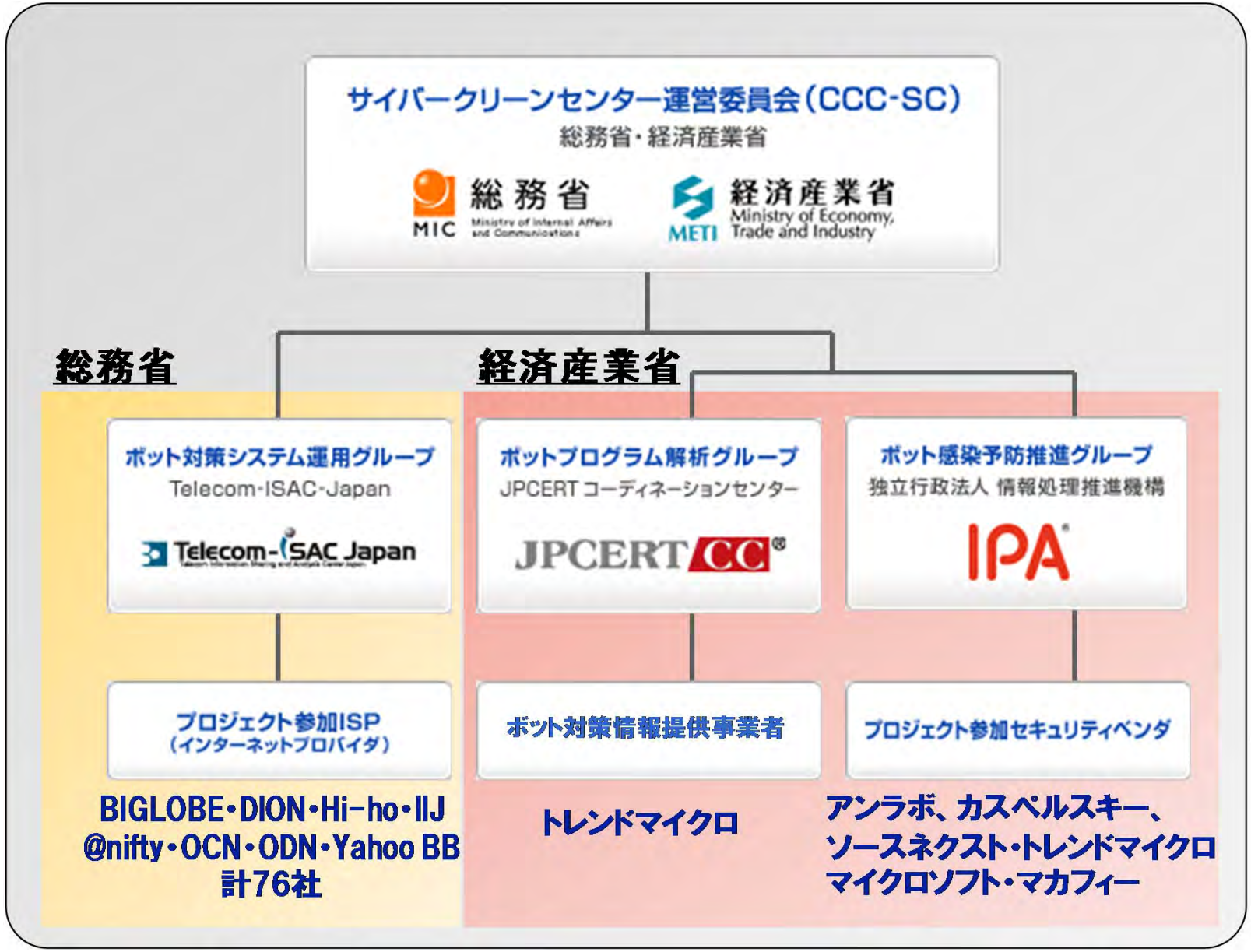
4 対策サイトにアクセス

5 ボット駆除ツール（CCCクリーナ）のダウンロード

CCCクリーナを使用し駆除を行うと共に再感染防止の対策を行う。

[2006～2010年度の総予算額：3,636百万円]

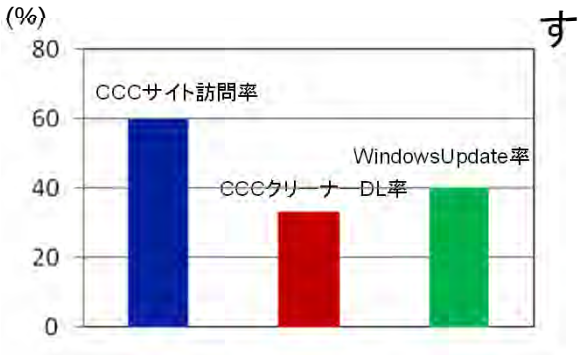
ボット対策プロジェクト②～体制～



ボット対策プロジェクト③～成果～

国内ボット感染率はプロジェクト開始当初の約3%から約0.6%まで減少したが。。。

	2007年5月	2010年12月
注意喚起メール（当月）	22,674通	2,402通
注意喚起メール（累積）	54,209通	533,737通
CCCクリーナーDL率	29%（累積）	33%（累積）



注意喚起を受けてCCCクリーナー(ボットウイルス駆除ツール)をダウンロードする人は33%前後で推移

注意喚起対応期間
（2007年2月～2010年12月）
注意喚起ユーザ数108,164

CCCサイト訪問率は6割、CCCクリーナーDL率は3割強

リテラシーを磨かずにインターネットを利用しているユーザーが悪いのか？

- 相談しても、たらいまわしにされる
- 身近に正しい情報を与えてくれる人がいない

ユーザーサポート面

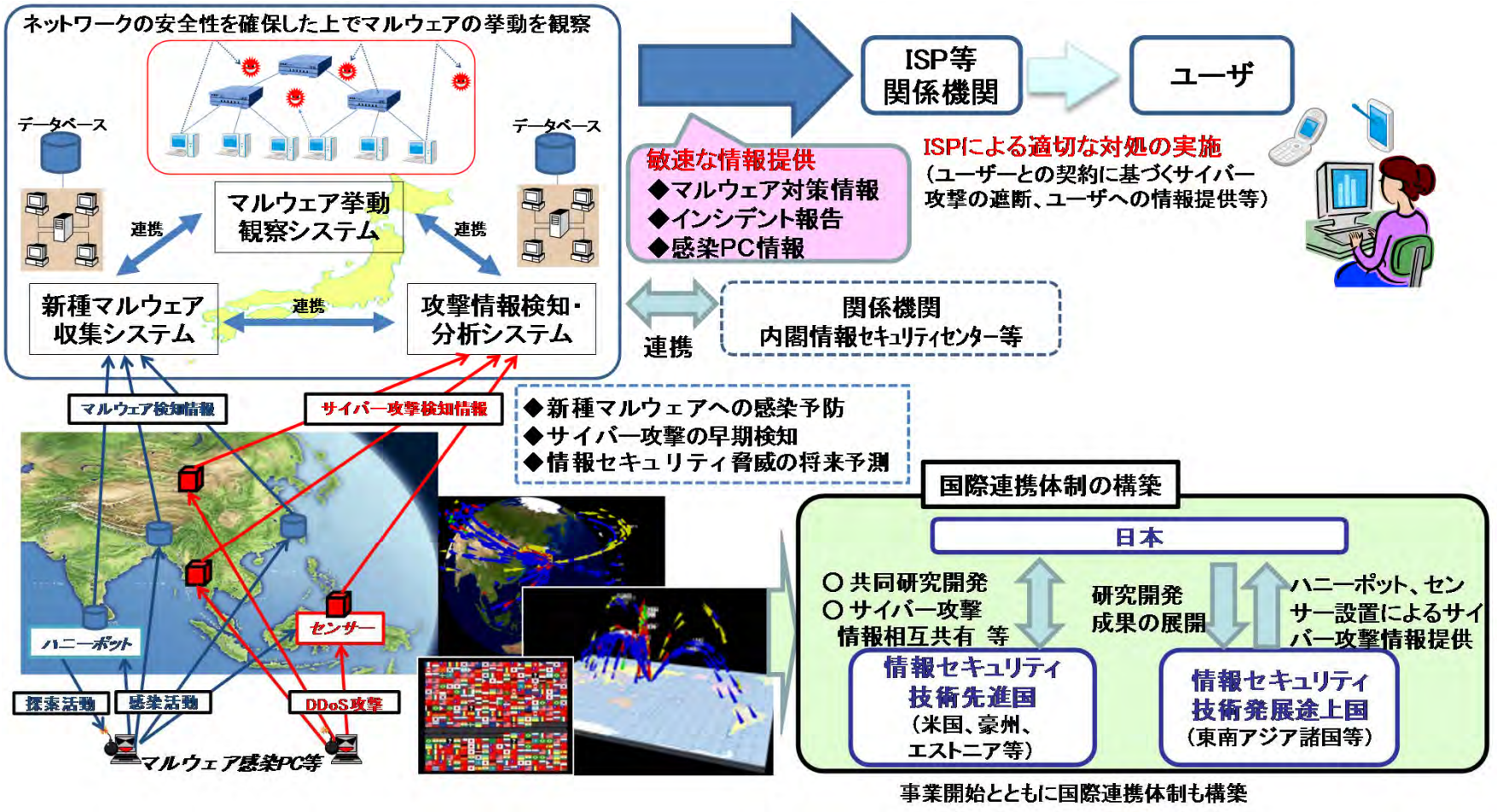
- ネットワークが未完成であり、一定レベルの品質を供給者側で維持する必要がある

技術面

ボット対策プロジェクト④～後継施策～

国際連携によるサイバー攻撃予知・即応技術の研究開発（2011年度予算額：629百万円）

◆サイバー攻撃に関する情報収集ネットワークを国際的に構築し、米国、豪州、APEC諸国をはじめとする諸外国と協力して、サイバー攻撃に対抗するための研究開発を実施し、日本におけるサイバー攻撃等のリスクを軽減。

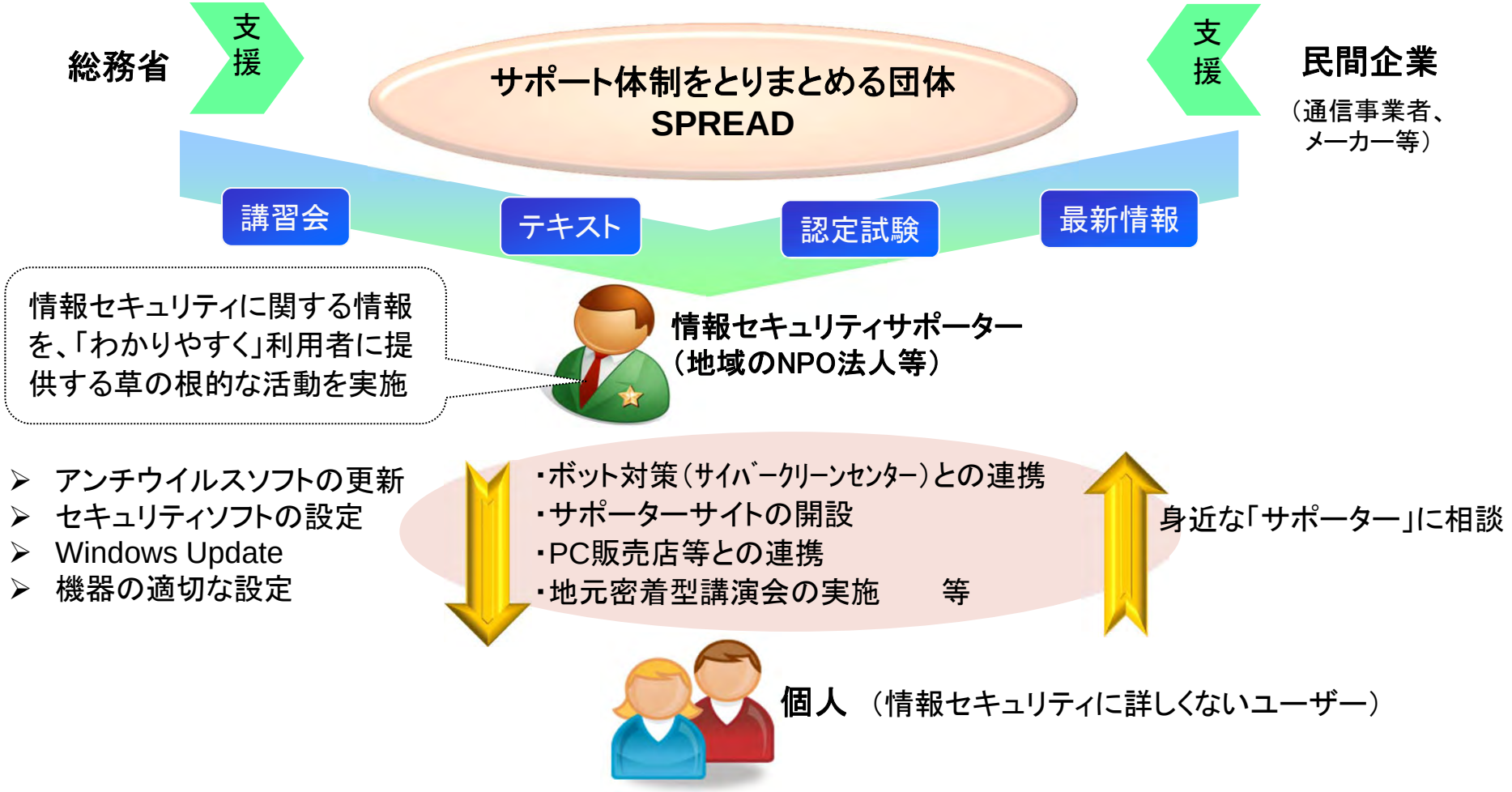


事業開始とともに国際連携体制も構築

地域活動を通じた個人のセキュリティ水準向上

総務省プロジェクト

◆地域NPO法人等と連携して、情報セキュリティ対策をサポートする人材育成や体制整備を支援



研究開発・インシデントの分析

独立行政法人　情報通信研究機構（NICT）

◆サイバー攻撃をリアルタイムに検知・分析する技術の研究開発

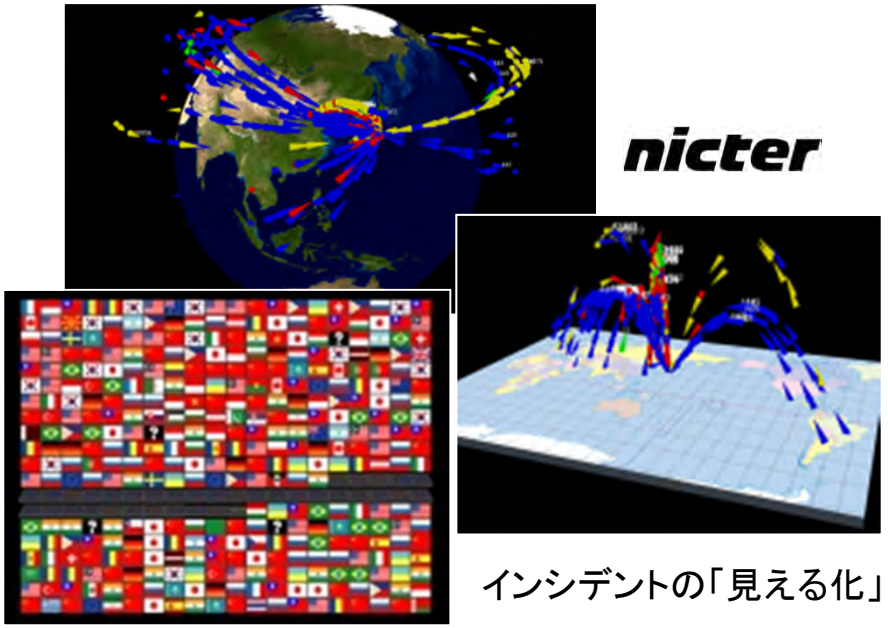
これまでの主な成果

- ◆ 大規模なインターネット観測とマルウェアの完全自動解析を行い、サイバー攻撃とそれを引き起こしているマルウェアの特定を可能とするインシデント分析センター「*nicter*」を開発
- ◆ サイバー攻撃のリアルタイムの「見える化（可視化）」を行い、早期検知、高精度分析、実効的な対策を実現

〈成果の展開〉

◆Telecom-ISAC及びセキュリティベンダーとの連携を通して、攻撃・インシデント情報の共有を推進。また、ITU-T及びISO/IECなどの国際標準化活動にも貢献

インシデント分析センター



インシデントの「見える化」

総務省
MIC Ministry of Internal Affairs and Communications

3．今後の課題

- サイバー攻撃の影響範囲の拡大
  - インターネット以外への影響
  - サイバー戦争？
- スマートフォンの急速な普及
  - セキュリティ確保のための役割分担
  - 利用者の意識啓発
- 「安心」と「安全」は別物？

サイバー攻撃の影響範囲の拡大①

サイバー戦争？

◆「陸・海・空」に加えて、20世紀後半に「宇宙」が交戦空間として意識されたところ、近年はインターネットなど「サイバー」の安全保障に注力する国も増加している

◆「サイバー戦争」の定義や認識等が曖昧な状態であるが、各国・政府機関が安全を確保するべく、それぞれの取り組みを進めている

〈サイバー空間の攻撃が「サイバー戦争」に該当するかどうかの判断基準とされる例〉

- **主体**：攻撃が国家によって実行されたか、又は国家支援で行われたか
- **被害**：攻撃によって被害が発生したか　国民への影響、社会経済活動への影響？
- **動機**：攻撃に政治的な動機があるかどうか　偶発的な事故か？
- **水準**：攻撃に特殊な手法を用いたり、緻密な計画があったか

朝日新聞（2010年10月4日GLOBE特集記事）

サイバー戦争：それは脅威なのか

CYBER WAR

一体」と司令官が宣言

「中国から侵入」と報告書

過去の国会での答弁事例

衆議院・武力攻撃事態への対処に関する特別委員会　H14.5.29

○前原誠司委員：サイバーテロ、サイバーウオーがあって、金融とか電力、水道、交通などの経済活動が壊滅的な打撃を受けて（・・中略・・）死傷者がたくさん出ている、つまりは、極めて日本に対してのダメージが与えられている、この場合は武力攻撃事態と認定されるんですか、どうなんですか。

○福田康夫官房長官：ある事態が武力攻撃事態に該当するか否か、あるいは自衛権を発動し得るか否かということは、個別具体的な状況を踏まえて判断すべきものでありまして、今のような仮定の問題について断定的に申し上げるのは、これは適当ではないと思います。したがいまして、一般論として申し上げますけれども、サイバー攻撃のようなものが武力の行使に当たるか否かについて、現状は、その法的性格について国際的には定説がありません。このため、これが武力攻撃事態に該当するかどうかは、現段階で確たることを申し上げることは困難であります。

サイバー攻撃の影響範囲の拡大②

2010年

危ないウィルスの認識

→ 2010年に入り、Win32.STUXNETと呼ばれていたウィルス（通称ｽﾀｯｸｽﾈｯﾄ）が、パソコンでの動きとは別に、USB等を介して特定の制御システム（独Siemens社製）に侵入しようとすること等が判明し、警告された

イランの原子力発電所でのウィルス発見報道

9月

→ 国営通信社が、ロシアの支援を受けて建設中のブシェール原子力発電所等でウィルスが発見されたことを報道

イランICT省大臣「今のところ深刻な被害は出ていない」とコメント

→ 諸外国でも感染が確認されたが、60%以上がイランに集中。「イラン原発を狙ったサイバー攻撃」との報道相次ぐ

イランの捜査当局が犯人逮捕とのマスコミ報道

→マスコミ報道があるも、犯人の身元情報等は不明

10月

日本国内でも63件のウィルス感染パソコンが発見された旨の報道

→制御システムへの感染は確認されていない

Google vs. 中国政府

2010年

1月
- グーグル社は、政府によるインターネット検閲やシステム侵入等が続く場合は、中国（google.cn）から撤退する意志を表明
- クリントン国務長官は「インターネットの自由」の声明を発表。中国、チュニジア、ウズベキスタン等での検閲政策等を批判
- 中国政府は、企業の国内法制度の遵守、侵入への関与無し等を主張

3月
- グーグル社は撤退（香港サイト（.hk検閲なし）へ自動転送）

7月
- グーグル社は検閲のない「音楽」「翻訳」「ショッピング」の3サービスを中国（google.cn）で復活（.hkへ手動転送）


グーグル
自主制限を一部解除
中国「検閲」に対抗か

毎日新聞（1月14日）


グーグルへのサイバー攻撃元
中国政府関係者か
米情報会社が調査結果 使用サーバー特定

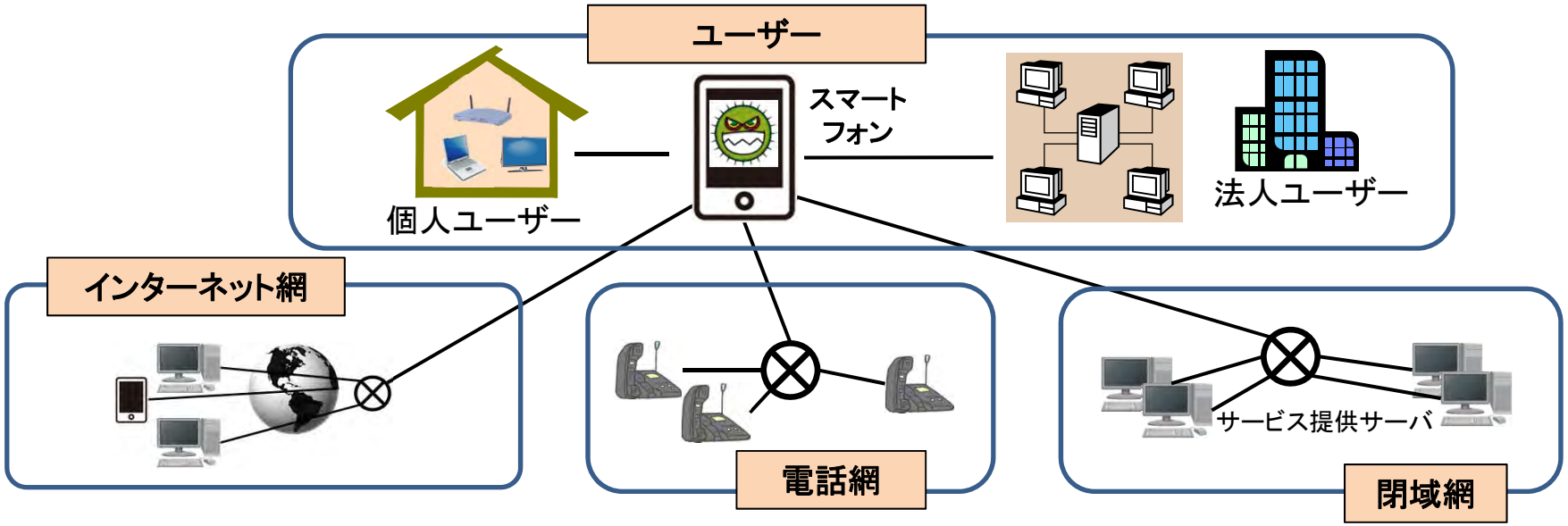
東京新聞（1月15日）


米国務長官「ネット検閲拒否を」
グーグル問題 中国に調査要求

毎日新聞（1月22日）

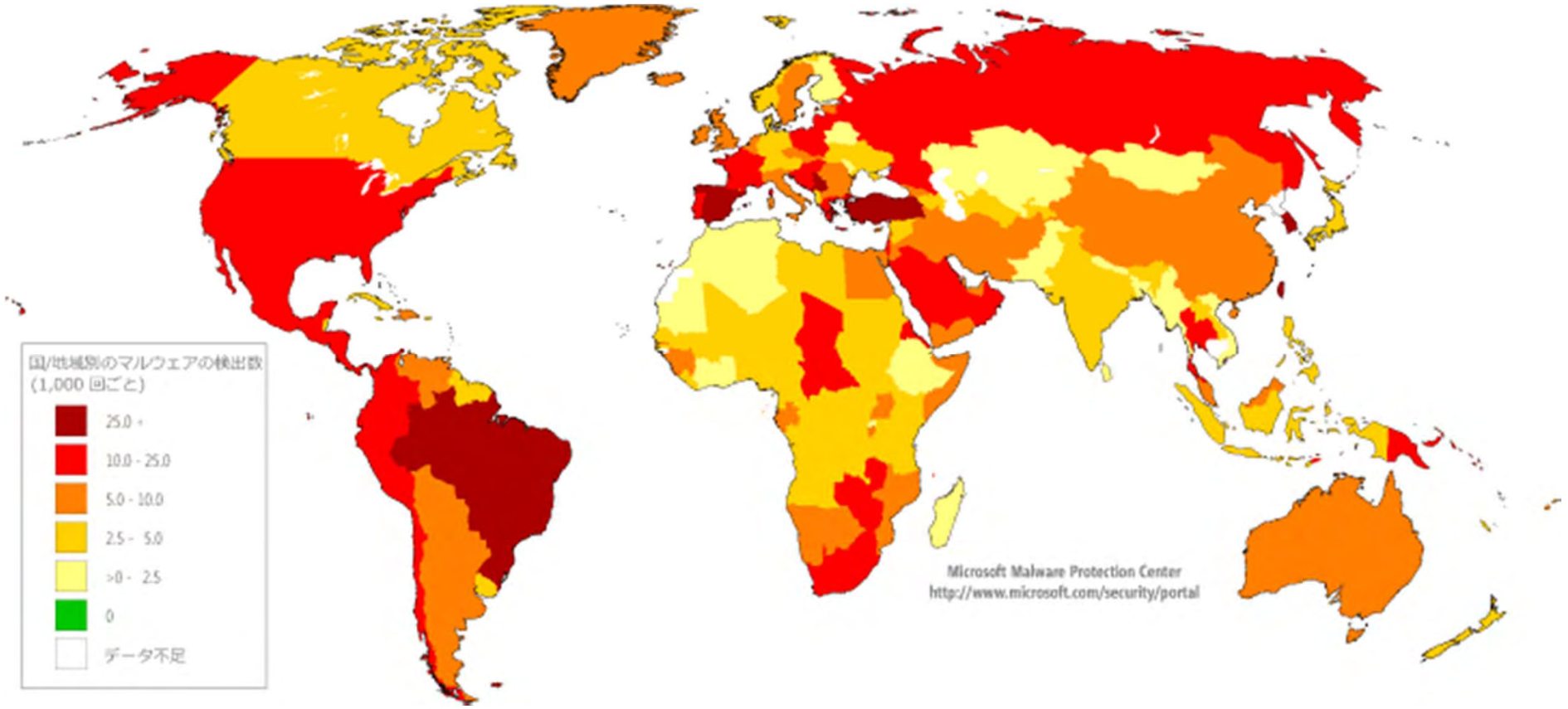
スマートフォンの急速な普及

- 「スマートフォン」の特徴
  - PCと同等の機能を有する高機能携帯電話
  - アプリケーションのインストールによる機能追加が可能
- セキュリティ確保のための役割分担
  - 携帯電話事業者、OSベンダー、端末ベンダー、アプリ提供者、ISPとプレーヤーは多岐に渡る
  - インターネットへは携帯電話事業者のネットワークまたはISPのネットワークを通じて接続
- 利用者の意識啓発
  - 「高機能な携帯電話」という意識
    - PC利用者に対する啓発（OSのアップデート、ウイルスソフトの利用等）と同様に、スマートフォン利用者に対しても啓発が必要ではないか



「安心」と「安全」は別物?①

日本のマルウェア感染率は世界最低水準

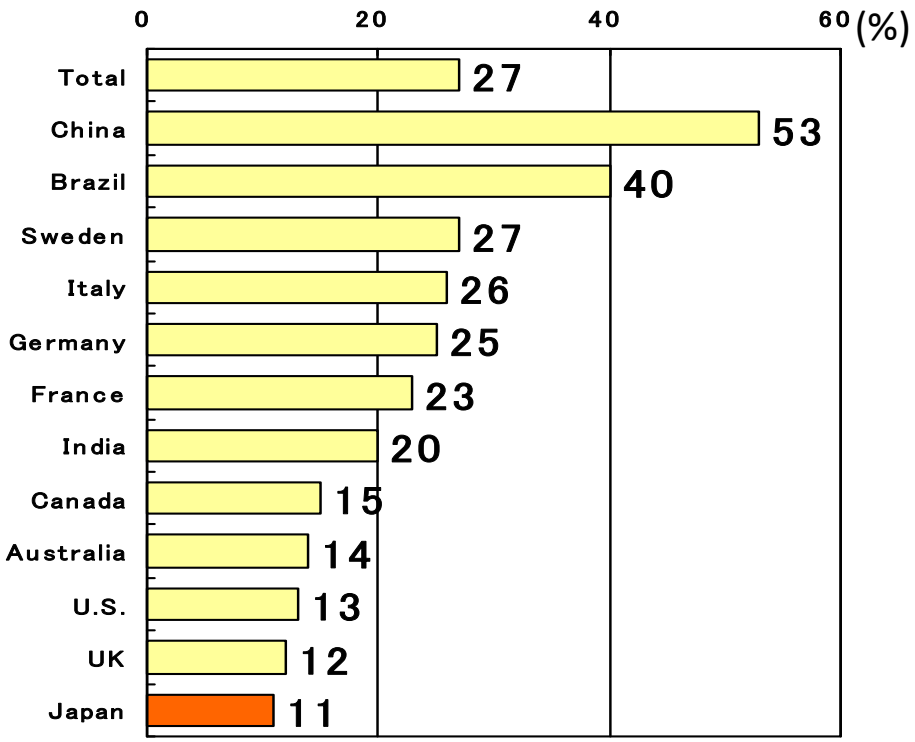


マイクロソフト社　セキュリティ・インテリジェンス・リポート　2010年第二四半期

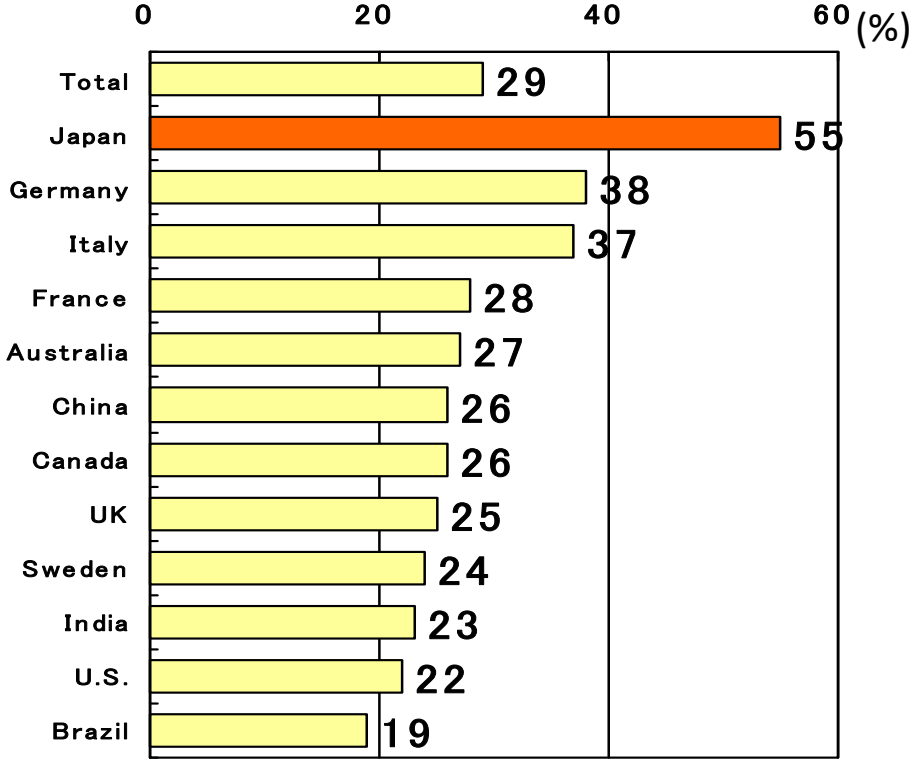
「安心」と「安全」は別物?②

セキュリティの「安心感」に関する国際比較

自分のコンピュータに侵入されたことがある



自分個人の情報セキュリティに不安がある
（「不安」と答えた割合%）



シマンテック社: Norton Online Living Report 2009 Survey Data (March 17, 2009)